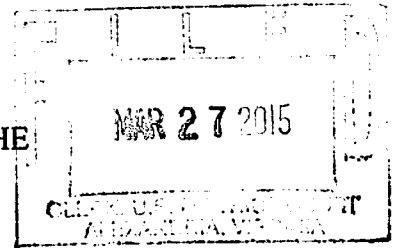


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA



Alexandria Division

UNITED STATES OF AMERICA

v.

MUSADDIQ ISHAQ,

Defendant.

)
)
) CRIMINAL NO. 1:15MJ173
)
)
)

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANT

I, Gershon Ross, being duly sworn, depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the United States Department of Homeland Security (DHS) and have been employed in that capacity since November 2011 and am currently assigned to the Office of the Chief Security Officer, Internal Security and Investigations Division (ISID). I have been a Special Agent / Investigator for the U.S. government for over 22 years. My current responsibilities include the investigation of violations of United States laws, including the misuse of government computer systems, and unauthorized access and disclosure of sensitive or classified information.

2. This affidavit does not contain every detail of every aspect of this investigation, but rather sets forth those facts that I believe are necessary to demonstrate probable cause to believe that, within the Eastern District of Virginia and elsewhere, MUSADDIQ ISHAQ conspired with Muneeb Akhter, Sohaib Akhter, and others known and unknown, to knowingly and with intent to defraud traffic in and use one or more unauthorized access devices during a one-year period, and by such

conduct obtained things of value aggregating \$1,000 or more during that period, said conduct affecting interstate commerce, in violation of 18 U.S.C. §§ 1029(a)(2) and (b)(2) (conspiracy to commit access device fraud).

3. The information in this affidavit is based on information obtained during the course of a criminal investigation conducted by DHS and includes evidence obtained from search warrants, records obtained from companies in response to subpoenas, and interviews. Since this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known regarding this investigation.

SUMMARY

4. Based on my investigation, there is probable cause to believe that ISHAQ is involved in a scheme to defraud in which he and his coconspirators obtained credit card account information belonging to other persons and used this information to make purchases throughout the country. In particular, ISHAQ and his coconspirators obtained compromised credit card numbers, which are unauthorized access devices. ISHAQ and his coconspirators used and conspired to use the unauthorized devices to make purchases, including airline tickets and other merchandise, at stores in the Eastern District of Virginia and elsewhere.

STATEMENT OF FACTS SUPPORTING PROBABLE CAUSE

5. On June 25, 2014, I was notified that DHS contract employee Muneeb Akhter had boasted to coworkers about hacking several e-commerce sites, including Subway, Starbucks, and an unspecified airline. On June 26, 2014, I questioned Muneeb Akhter in a noncustodial setting at the DHS St. Elizabeths campus in Washington, DC. In a sworn statement, Muneeb Akhter told me that he had created a computer code to gain unauthorized access to several e-commerce websites

including K-Mart, Shell Gasoline, Whole Foods, Starbucks, and Dunkin Donuts. He stated that his computer code allowed him to add funds to gift cards without having to expend any actual funds. He admitted to using gift cards for personal use, as well as fraudulently placing funds on gift cards for others, also without expending funds.

6. On July 24, 2014, I and other law enforcement officers executed a federal search warrant at Muneeb Akhter's residence, 7510 Chancellor Way, Springfield, VA, in the Eastern District of Virginia. Pursuant to the search warrant, I and other law enforcement officers seized several items including computers and cell phones.

7. Forensic analysis of a T-Mobile LG cell phone recovered from the residence revealed numerous audio files of phone conversations that were stored in the phone's memory. During many of these recorded conversations, Muneeb Akhter, his brother Sohaib Akhter, and ISHAQ discussed their acquisition and possession of fraudulently obtained credit card numbers. The Akhter brothers and ISHAQ also discussed their use of credit card numbers and related account information, which they had fraudulently obtained from an e-commerce cosmetics company called Shea Terra Organics, to purchase goods and services.

8. On an audio recording dated June 5, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. On the recording, Sohaib Akhter informed ISHAQ that Muneeb Akhter was obtaining credit card numbers via e-mail from a program that Muneeb Akhter had inserted onto computer systems for Shea Terra Organics. Specifically, Sohaib Akhter stated that Muneeb Akhter received twenty-four credit card numbers using a computer program that automatically e-mailed credit card numbers to Muneeb Akhter. Based on my training, experience, and knowledge of the

investigation, I believe that Muneeb Akhter and ISHAQ were discussing the theft of credit card numbers belonging to customers who purchased goods on Shea Terra's website.

9. My investigation revealed that ISHAQ's mother was the registered agent for Shea Terra Organics.

10. On an audio recording dated May 27, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. ISHAQ told Sohaib Akhter that he needed two credit card numbers to make a purchase. ISHAQ asked Sohaib Akhter for the login and password to a database file. He also told Sohaib Akhter not to worry and that they can get fifty more credit card numbers.

11. On an audio recording dated May 28, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. Sohaib Akhter told ISHAQ that he thought Expedia "would definitely know cc fraud if they saw it" but that "they were fooled." ISHAQ asked Sohaib Akhter if "the flight" was purchased through Expedia. Sohaib Akhter replied that a flight, hotel, and rental car were all purchased through Expedia. ISHAQ commented that "we need to make hard cash using cc's" and suggested "we need to start using cards, especially with expiration dates coming soon." Based on information and belief, Akhter and ISHAQ's use of the term "cc" meant "credit card."

12. On an audio recording dated May 28, 2014, I identified voices belonging to Sohaib Akhter and Muneeb Akhter. Muneeb Akhter informed Sohaib Akhter that Muneeb Akhter would be delaying his return flight from California by a day. Sohaib Akhter asked Muneeb Akhter if he would be using any more credit cards to push back his flight. Muneeb Akhter responded that he would.

13. On an audio recording dated May 28, 2014, I identified voices belonging to Muneeb Akhter and Sohaib Akhter. Muneeb Akhter told Sohaib Akhter that they should tell others that they were able to hack an airline's system and could get free rides wherever they want.

14. On an audio recording dated May 28, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. ISHAQ told Sohaib Akhter “don’t worry about wasting cards” because “we can get cards whenever we want.” Based on my training, experience, and investigation of this case, I believe Sohaib Akhter and ISHAQ were discussing the fact that they could acquire new credit card numbers and associated information from Shea Terra at will.

15. On an audio recording dated June 3, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. ISHAQ advised Sohaib Akhter that “cops are showing up at your house” and added “you need to erase everything! Every damn thing.” ISHAQ indicated that this was because his mother was “being a piece of shit” and had called the police “about hacking website and breaking into warehouse.” ISHAQ said, “My mom doesn’t understand. You guys can make any story up you want, that she was helping you guys, she came to you guys and asked you to hack her website, whatever, make it look like I’m being hacked.” ISHAQ added, “On your side, yes you actually did something wrong. On her side, yes she didn’t do shit wrong.” Sohaib Akhter commented, “I want to see them come to our house with a court subpoena.” ISHAQ responded, “Get ready to cover your ass.”

16. On an audio recording dated June 7, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. Sohaib Akhter asked ISHAQ if he would like to go to Busch Gardens the next day. ISHAQ responded “see if you can use cc’s to get Busch Gardens tickets. Try it.”

17. On an audio recording dated June 25, 2014, I identified voices belonging to Muneeb Akhter and Sohaib Akhter. Muneeb Akhter asked Sohaib Akhter if he had purchased a K-Mart gift card yet and if he had tried reloading it. Based on my training, experience, and investigation of this

case, I believe Muneeb Akhter and Sohaib Akhter were discussing adding value to K-Mart gift cards using fraudulently obtained credit card numbers.

18. On an audio recording dated June 26, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. Sohaib Akhter and ISHAQ discussed purchasing reloadable gift cards from K-Mart and adding value to them using credit cards. They agreed to meet at a local Sears because the K-Mart gift cards could also be used there.

19. On an audio recording dated June 26, 2014, I identified voices belonging to Muneeb Akhter and Sohaib Akhter. Muneeb Akhter asked Sohaib Akhter if the K-Mart cards worked. Sohaib Akhter indicated that the cards were working and that he had made purchases for items including “tablets” and “gas cards.”

20. On an audio recording dated July 15, 2014, I identified voices belonging to Sohaib Akhter and ISHAQ. Sohaib Akhter explained to ISHAQ that the computer program that Muneeb Akhter described to DHS agents does not exist and was simply a cover for their true activity.

21. Pursuant to Grand Jury subpoena requests, I obtained records relevant to my investigation from Expedia.com, United Airlines, and U.S. Airways. I identified approximately five flights for which Muneeb Akhter or his grandmother was listed as a passenger. The flights were paid for using credit card numbers and associated personal identifiers—including names and addresses—that belonged to individuals other than Muneeb Akhter, Sohaib Akhter, their grandmother, and ISHAQ.

22. For one flight, records I obtained from Expedia.com indicated that “Muneeb Akhter” booked a round trip airline ticket from Washington, DC, to Los Angeles, CA, departing May 27, 2014, on U.S. Airways flights 1840 and 721 and returning May 29, 2014, on U.S. Airways flights

1832 and 1960. Records I obtained from U.S. Airways confirmed the purchase, with Muneeb Akhter listed as the passenger. A MasterCard credit card number ending in 6665 was used to make the purchase. The card holder's name was J.R., with an address in Elkland, PA. The total amount charged to that card for the airline ticket was \$465.

23. I contacted J.R. telephonically and she stated that the airline ticket was purchased without her knowledge or authority and that the credit card account had subsequently been closed. J.R. also stated that, prior to the fraudulent charge, she had purchased items from the Shea Terra Organics website.

24. During his trip from May 27, 2014, to May 29, 2014, Muneeb Akhter reserved a hotel room at the Viceroy Hotel in Santa Monica, CA, and a rental car from Dollar Rent a Car. The charge for the hotel was \$771.84 and the charge for the rental car was \$45.98, for a total charge of \$817.82. Of this amount, an additional \$176.41 was charged to the MasterCard credit card number ending in 6665 belonging to J.R. The remaining \$641.41 was charged to a MasterCard credit card number ending in 1681. The card holder's name was D.F., with an address in Philadelphia, PA.

25. During the course of my investigation, I determined that multiple online purchases of goods and services were made on behalf of both Muneeb Akhter and Sohaib Akhter using credit cards belonging to individuals other than the Akhter brothers. These goods and services included, but were not limited to, purchases from: online auction sites; an online printing company based in Nevada; a sporting goods retailer located in West Virginia; a food delivery service that makes deliveries in Northern Virginia; an information technology certification research and education organization located in Maryland; a computer company located in Texas; and information technology-related conferences that took place in Washington, DC.

26. Pursuant to a Grand Jury subpoena request, I obtained records of deliveries to the address 7510 Chancellor Way, Springfield, VA, from United Parcel Service. Based on my investigation, I determined that both Sohaib Akhter and Muneeb Akhter reside at that address. Relevant items delivered to the residence include:

- A. HP ENVY Laptop – Delivered on April 14, 2014 – Value \$780.99
- B. Toshiba Chromebook – Delivered on April 15, 2014 – Value \$306.90
- C. Amazon Kindle Fire Tablet – Delivered on April 15, 2014 – Value \$131.99
- D. HP Wireless Printer – Delivered on April 23, 2014 – Value \$131.99

27. I obtained records related to the purchase of the items listed in Paragraph 26 from the online auction website Deal Dash. These records indicated that fraudulently obtained credit cards were used to buy “bid units” on Deal Dash. Those “bid units” were used to win auctions for the items listed in Paragraph 26, which Deal Dash ultimately purchased and sent to the Akhter residence.

28. Many of the fraudulent purchases identified above were made after the execution of the federal search warrant in July 2014.

29. Pursuant to a Grand Jury subpoena request, I obtained records and information related to an e-mail account associated with Sohaib Akhter. A November 20, 2014, e-mail from ISHAQ to Sohaib Akhter contained a list of names and associated “billing” and “shipping” information, including addresses, phone numbers, and credit card numbers. One of the names listed was S.Y. with an address in Greenville, SC, and a Visa card ending in 5964.

30. The e-mail account also included a December 1, 2014, e-mail from Dell, Inc., a Texas-based computer company, to Sohaib Akhter. The e-mail indicated that Dell was processing an order for an Inspiron 15 laptop computer, for a total cost of \$871.91. The e-mail began with the

salutation “[S.Y.], thanks again for your order!” The shipping information indicated that the laptop would be sent to “Sohaib Akhter” at “7510 Chancellor Way, Springfield, VA 22153.” The billing information listed S.Y.’s address in Greenville, SC. The next day, December 2, 2014, Dell, Inc. sent two e-mails to Sohaib Akhter, indicating that the order had been cancelled due to security concerns relating to the credit card used to place the order.

31. I contacted S.Y.’s wife E.Y. telephonically. She stated that in December 2014 she received a call from Dell asking if she had placed an order for a computer. E.Y. informed Dell that neither she nor S.Y. had ordered a computer. She then closed the credit card account. E.Y. also stated that, prior to the fraudulent charge, she had purchased items from Shea Terra Organics.

32. Information provided to me by the Fairfax County Police Department indicated that in December 2014, Muneeb Akhter received shipments of archery equipment and registered for an information technology course. I contacted representatives at the companies who sold those goods and services. The representatives indicated that the goods and services had been purchased using credit cards belonging to individuals other than Muneeb Akhter, Sohaib Akhter, and ISHAQ. The value of those goods and services was \$592.94 for the archery equipment, \$116.55 for shipment of course material for the information technology course, and \$5,350.00 for registration for the information technology course.

33. Based on my investigation, the total amount charged for goods and services, between in or around April 2014 to in or around January 2015, which I attribute to fraudulent credit card activity conducted by Muneeb Akhter, Sohaib Akhter, and ISHAQ, exceeded \$25,000.00.


34. I identified and contacted approximately eight of the holders of the fraudulently used credit cards, whose names are J.R., D.F., C.W., A.B., L.L., A.H., L.P., and S.Y., or one of their

associates. Each card holder or their associate confirmed that he or she was a victim of credit card fraud. Each card holder or associate also confirmed that he or she made at least one online purchase from Shea Terra Organics using a credit card that was later associated with fraudulent activity.

35. Based on my training and experience in conducting criminal investigations, I believe that ISHAQ's conduct affected interstate commerce. ISHAQ used and conspired to use credit card accounts of financial institutions that operate throughout the United States at stores that operate in multiple states. Further, when an unauthorized credit card is used, it causes a financial transaction between the bank and other business entities such as the issuing bank for the card and the clearing center processing the transactions. In addition, as described in Paragraphs 25 and 30, ISHAQ conducted and conspired to conduct this scheme in multiple states, including Nevada, West Virginia, Maryland, and Texas.

CONCLUSION

36. Based on the foregoing, there is probable cause to believe that, within the Eastern District of Virginia and elsewhere, MUSADDIQ ISHAQ conspired with Muneeb Akhter, Sohaib Akhter, and others known and unknown, to knowingly and with intent to defraud traffic in and use one or more unauthorized access devices during a one-year period, and by such conduct obtained things of value aggregating \$1,000 or more during that period, said conduct affecting interstate commerce, in violation of 18 U.S.C. §§ 1029(a)(2) and (b)(2) (conspiracy to commit access device fraud).


Special Agent Gershon Ross
Department of Homeland Security

Sworn and Subscribed before me this 27th day of March, 2015.

Michael S. Nachmanoff
United States Magistrate Judge

The Honorable Michael S. Nachmanoff
United States Magistrate Judge

Criminal Case Cover Sheet**U.S. District Court**

Place of Offense: Under Seal: Yes ___ No ☒ Judge Assigned: _____
 City _____ Superseding Indictment _____ Criminal Number: _____
 County/Parish Fairfax Same Defendant _____ New Defendant ☒
 Magistrate Judge Case Number 1:15MJ173 Arraignment Date: _____
 Search Warrant Case Number _____
 R 20/R 40 from District of _____
 Related Case Name and No: _____

Defendant Information:

Juvenile -- Yes ___ No ☒ FBI # _____
 Defendant Name: MUSADDIQ ISHAQ Alias Name(s) _____
 Address: 41350 Springfield Lane, Leesburg, VA 20175
 Employment: _____
 Birth date 11/15/1993 SS# 230-69-3581 Sex M Def Race _____ Nationality U.S. Place of Birth _____
 Height _____ Weight _____ Hair Black Eyes Brown Scars/Tattoos _____
 Interpreter: ☒ No ___ Yes List language and/or dialect: _____ Automobile Description _____

Location Status:

Arrest Date _____
 ___ Already in Federal Custody as of _____ in _____
 ___ Already in State Custody ___ On Pretrial Release ☒ Not in Custody
☒ Arrest Warrant Requested ___ Fugitive ___ Summons Requested
 ___ Arrest Warrant Pending ___ Detention Sought ___ Bond _____

Defense Counsel Information:

David Benowitz
 Name: Price Benowitz LLP ___ Court Appointed Counsel conflicted out: _____
 409 7th St NW #222,
 Address: Washington, DC 20004 ☒ Retained _____
 Telephone: 202-417-6000 ___ Public Defender Federal Public Defender's Office conflicted out: _____

U.S. Attorney Information:

SAUSA John Taddei Telephone No: 703-299-3738 Bar # _____

Complainant Agency, Address & Phone Number or Person & Title:

Special Agent Gershon Ross, Department of Homeland Security

U.S.C. Citations:

	<u>Code/Section</u>	<u>Description of Offense Charged</u>	<u>Count(s)</u>	<u>Capital/Felony/Misd/Petty</u>
Set 1	<u>18 U.S.C. §§ 1029(a)(2) and (b)(2)</u>	<u>Conspiracy to Commit Access Device Fraud</u>	<u>1</u>	<u>Felony</u>
Set 2	_____	_____	_____	_____
Set 3	_____	_____	_____	_____

(May be continued on reverse)

Date: 3/27/15 Signature of SAUSA: _____

REDACTED**Criminal Case Cover Sheet****U.S. District Court**

Place of Offense: _____ **Under Seal:** Yes ___ No **X** **Judge Assigned:** _____
City _____ **Superseding Indictment** _____ **Criminal Number:** _____
County/Parish Fairfax **Same Defendant** _____ **New Defendant** **X** _____
Magistrate Judge Case Number 1:15MJ173 **Arraignment Date:** _____
Search Warrant Case Number _____
R 20/R 40 from District of _____
Related Case Name and No: _____

Defendant Information:

Juvenile --Yes ___ No **X FBI #** _____
Defendant Name: MUSADDIQ ISHAQ **Alias Name(s)** _____
Address: Leesburg, VA _____
Employment: _____
Birth date xx/xx/1993 **SS#** xxx-xx-3581 **Sex** M **Def Race** _____ **Nationality** U.S. **Place of Birth** _____
Height _____ **Weight** _____ **Hair** Black **Eyes** Brown **Scars/Tattoos** _____
Interpreter: X **No** ___ **Yes** **List language and/or dialect:** _____ **Automobile Description** _____

Location Status:

Arrest Date _____
 ___ **Already in Federal Custody as of** _____ **in** _____
 ___ **Already in State Custody** ___ **On Pretrial Release** **X** **Not in Custody** _____
X **Arrest Warrant Requested** ___ **Fugitive** ___ **Summons Requested** _____
 ___ **Arrest Warrant Pending** ___ **Detention Sought** ___ **Bond** _____

Defense Counsel Information:

Name: David Benowitz **Court Appointed** ___ **Counsel conflicted out:** _____
Price Benowitz LLP
409 7th St NW #222,
Address: Washington, DC 20004 **X** **Retained** _____
Telephone: 202-417-6000 ___ **Public Defender** **Federal Public Defender's Office conflicted out:** _____

U.S. Attorney Information:

SAUSA John Taddei **Telephone No:** 703-299-3738 **Bar #** _____

Complainant Agency, Address & Phone Number or Person & Title:

Special Agent Gershon Ross, Department of Homeland Security

U.S.C. Citations:

	<u>Code/Section</u>	<u>Description of Offense Charged</u>	<u>Count(s)</u>	<u>Capital/Felony/Misd/Petty</u>
Set 1	18 U.S.C. §§ 1029(a)(2) and (b)(2)	Conspiracy to Commit Access Device Fraud	1	Felony
Set 2				
Set 3				

(May be continued on reverse)

Date: 3/27/15 **Signature of SAUSA:** 